



Release Notes for Cisco 3200 Series Router

Revised: February 25, 2008, 78-13975-18

Introduction

These release notes provide information on accessing the latest documentation and technical information available for the Cisco 3200 Series Router.

Contents

- [New Features, page 1](#)
- [Caveats, page 4](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation and Submitting a Service Request, page 12](#)

New Features

The following list identifies the new features in this release:

- [Multiple Client Profile, page 2](#)
- [EAP-TLS, page 2](#)
- [Interoperability with Cisco LWAPP Access Points, page 2](#)
- [New 5-GHz WMIC \(Cisco 3205\), page 2](#)



Multiple Client Profile

The Multiple Client Profile (MCP) feature allows a Cisco 3201 Wireless Mobile Interface Card (WMIC) in a client station role (workgroup bridge, non-root, universal workgroup bridge) to maintain multiple client profiles—one profile for every configured service set identifier (SSID). Every profile contains authentication types and cipher suites for the corresponding SSID. This use of a profile-based system allows the various SSIDs to maintain prioritization.



Note

The MCP feature is available only on the 2.4-GHz Cisco 3201 WMIC.

EAP-TLS

Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) is now supported by the 4.9-GHz Cisco 3202 WMIC and the 5-GHz Cisco 3205 WMIC.

EAP-TLS is a specific type of EAP. EAP-TLS is already supported by the Cisco 3201 WMIC.

Interoperability with Cisco LWAPP Access Points

Functioning in the workgroup bridge station role, the 2.4-GHz Cisco 3201, 4.9-GHz Cisco 3202, and 5-GHz Cisco 3205 WMICs can interoperate with the following Cisco mesh access points:

- Cisco 1522 Mesh Access Point
- Cisco 1524 Mesh Access Point
- Cisco 1242 Access Point
- Cisco 1250 Access Point

New 5-GHz WMIC (Cisco 3205)

This release features a new 5-GHz Cisco 3205 WMIC. This WMIC can be configured in any of the following modes:

- Root bridge
- Non-root bridge
- Workgroup bridge
- Access point

When configured in a workgroup bridge station role, the WMIC can associate to a Cisco 1522 Mesh Access Point, serving as a wireless backhaul for an in-vehicle mobile network.

The Cisco 3205 WMIC can also be used to set up point-to-point, or point-to-multipoint bridges. The new 5-GHz radio in this WMIC improves throughput at lower temperatures.

Supported Channels

North America customers can use only the following frequencies in the 5.725- to 5.850-GHz band:

- 5745 MHz (149)
- 5765 MHz (153)
- 5785 MHz (157)
- 5805 MHz (161)
- 5825 MHz (165)

To comply with FCC regulations, use of the following frequencies is prohibited in North America:

- 5.250 to 5.350 GHz: 5260 MHz (52), 5280 MHz (56), 5300 MHz (60), 5320 MHz (64)
- 5.470 to 5.725 GHz: 5500 MHz (100), 5520 MHz (104), 5540 MHz (108), 5560 MHz (112), 5580 MHz (116), 5600 MHz (120), 5620 MHz (124), 5640 MHz (128), 5660 MHz (132), 5680 MHz (136), 5700 MHz (140)

For C3205 ETSI, the following channels are supported:

- 5500 MHz (channel 100)
- 5520 MHz (channel 104)
- 5540 MHz (channel 108)
- 5560 MHz (channel 112)
- 5580 MHz (channel 116)
- 5600 MHz (channel 120)
- 5620 MHz (channel 124)
- 5640 MHz (channel 128)
- 5660 MHz (channel 132)
- 5680 MHz (channel 136)
- 5700 MHz (channel 140)

Caveats

This section contains the information for [Opened Caveats - Release 12.4\(3\)JK](#).

Opened Caveats - Release 12.4(3)JK

CSCsk13961 CISCO-DOT11-IF-MIB : Few object shows wrong value in snmp query

Symptom The following mib objects show wrong values for Cisco 1310, Cisco 3201, Cisco 3202, and Cisco 3205 radios: cd11IfAssignedSta, cd11IfClientCurrentTxPowerLevel1. And the following mib objects show wrong values for Cisco 3205 radios: cd11IfClientTxPowerLevel5 and cd11IfErpOfdmTxPowerLevel5.

Conditions Returns wrong values for the radios. Need to update the IF-MIB for the radios.

Workaround There is no workaround.

CSCsl111160 IOD: Trackbacks displayed during stress test

Symptom During stress traffic test (e.g. Smartbit traffic, cpu of UUT is at 98%), AP and wgb can display some tracebacks related to memory fragmentation and memory allocation.

Conditions This only occurs on stress traffic test when using Smartbit.

Workaround There is no workaround.

CSCsl42568 WMIC failed to associate using authentication shared

Symptom Cisco 3202 / Cisco 3205 Wireless MICs fail to associate via authentication shared using 12.4(3)JK release image.

Conditions Configure Cisco 3202 / Cisco 3205 Wireless MICs to be root and client devices with authentication method to be "authentication shared" under the SSID configuration.

Workaround Customer can use the more secured method "authentication open with WPA-PSK key management" to configure the Cisco 3202 and Cisco 3205.

CSCsm13296 WGB unable to re-associate after client triggers DFS on root Device

Symptom For FCC outdoor SKU, when all DFS channels are exhausted by radar detection on RB, non-dfs channel will be picked but cannot associate with WGB. However, if non-dfs channel is picked through channel CLI command, then it can associate with WGB.

Conditions Phase 1 release image would not have this problem since there will be no dfs channels on FCC outdoor SKU.

Workaround There is no workaround.

CSCsm31801 TKIP+ WPAV2+CCKM does not work

Symptom Association failure.

Conditions This occurs when the combination of "authentication key-management wpa version 2 cckm" + "encryption mode ciphers tkip" is configured.

Workaround There is no workaround. It is not a common configuration; customer can use aes instead of tkip.

CSCsm41374 Set fails & out of range value for some objects in Dot11-IF MIB objects

Symptom The following mib objects show wrong values for Cisco 1310 and Cisco 3201 radios: cd11IfSuppDataRatesPrivacyValue. The mib object, cd11IfModulationType, is a read-write object but throws "Not writable" error while doing setany operation for Cisco 1310 and Cisco 320x radios. The following mib objects can not be set correctly for Cisco 1310 and Cisco 3201 radios: cd11IfCiscoExtensionsEnable, cd11IfStationRole. The following mib object can not be set correctly for Cisco 1310 and Cisco 320x radios: cd11IfVlanEncryptKeyLen.

Conditions This issue is seen when using snmp get or set operations.

Workaround There is no workaround.

CSCsm41392 cd11IfMobileStationScanChannel returns unexpected line for channel 10

Symptom For object 'cd11IfMobileStationScanChannel', all the channels can be set through snmp except channel 10. The same behaviour is seen when setting 'cd11IfStationRole' (1, 5, 9). Also, you cannot set cd11IfMobileStationScanChannel to one octet of value of 0 to configure the radio and scan all the channels applicable to a particular regulatory domain.

Conditions This occurs while using snmp get or set operations with Cisco 1310, Cisco 3201, and Cisco 3202 radios.

Workaround There is no workaround.

CSCsm41453 Setany accepts the value but not set for few objects in dot11-IF MIB

Symptom Set operation accepts the value, but not set for the following objects:

```
cd11IfBridgeSpacing
cd11IfAuthAlgRequireEap
cd11IfAuxSsidAuthAlgRequireEap
cd11IfAuxSsidAuthAlgRequireMac
```

When "cd11IfAuxSsidAuthAlgRequireEap" is false, the below objects behaves erroneously:

```
cd11IfAuxSsidAuthAlgEapMethod
cd11IfAuxSsidAuthAlgMacMethod
cd11IfPhyDsssChannelAutoEnable
cd11IfAuxSsidWepPermuteAlg
cd11IfVlanSecurityVlanEnabled
cd11IfVlanSecurityCiphers
```

Set operation for following objects works fine when mode is wep(2). But not in cipher mode:

```
cd11IfVlanWepEncryptOptions
cd11IfVlanWepEncryptMic
cd11IfVlanWepEncryptKeyHashing
```

The operation works fine in both through CLI and SNMP when encapsulation is enabled on vlan and when encapsulation is not enabled, set operation accepts the value, but it is not set to cd11IfVlanPsPacketForwardEnable.

Conditions This issue is seen when using SNMP get or set operations.

Workaround There is no workaround.

CSCsm41504 Set operation successful but no reflection in CLI configuration

Symptom The mib object cd11IfPhyDsssMaxCompatibleRate returns wrong values. Also cd11IfPhyDsssMaxCompatibleRate cannot be set correctly from snmp. The following mib objects can be set from snmp, but does not reflect in configurations:

```
cd11IfAuxSsidAuthAlgRequireEap,
cd11IfAuxSsidAuthAlgRequireMac
cd11IfAuxSsidAuthAlgRequireMac
```

For object 'cd11IfDesiredSsidWepPermuteAlg', set operation is successful but there is no reflection in CLI configuration. Same behaviour for cd11IfAuxSsidWepPermuteAlg.

Conditions These issues are seen when using SNMP get or set operations.

Workaround There is no workaround.

CSCsm41553 cd11IfMobileStationListIgnore: set operation should not be allowed

Symptom The mib object, cd11IfMobileStationListIgnore, is not applicable to station roles (4, 2, 6) and should return false and set operation should be rejected, but it is not rejected. Also, if the value of "cd11IfMobileStationListIgnore" is true, and if we set the station role to one of (4, 2, 6), the object should populate as "false(2)", but it returns "true(1)".

Conditions These issues are seen when using SNMP get or set operations.

Workaround There is no workaround.

CSCsm41756 Set operation behaves erroneously for worldmode&country,DesiredBssidAddr

Symptom For object 'cd11IfWorldMode', only the value "none(1)" can be set through snmp set operation. The issue is that setting other two values "legacy(2)" or "dot11d(3)" causes the error: "Error code set in packet - COMMIT_FAILED_ERROR: 1". Setting cd11IfWorldModeCountry should show error when the world mode is not dot11d(3), but it accepts the command without changing the value. The other issue is that it also rejects setting the cd11IfWorldModeCountry when the world mode is dot11d(3). When the world mode is none(1), the object "cd11IfWorldModeCountry" does not reject country codes with the third character other than "O" or "I" or an ascii space character. For object "cd11IfDesiredBssidAddr", configuring through CLI and doing SNMP query works fine. However, setting value through SNMP behaves erroneously.

Conditions These issues are seen when using SNMP get or set operations.

Workaround There is no workaround.

CSCsm46488 CLI problem after convert LWAPP AP to autonomous AP

Symptom If customer has a Cisco 3201 LWAPP AP and converted it to Cisco 3201 autonomous AP with 12.4(3)JK release, the converted WMIC will have different encryption CLIs from the Cisco 3201 autonomous AP shipped from manufacture with the same release version. The converted WMIC will require customer to configure encryptions under dot11 interface while the normal autonomous AP with this version requires customer to configure encryptions under SSID configuration.

Conditions This only occurs when customer converts a LWAPP C3201 WMIC to autonomous C3201WMIC with 12.4(3) JK release.

Workaround Customers are not encouraged to convert a LWAPP Cisco 3201WMIC to autonomous Cisco 3201WMIC. The LWAPP WMIC may be sent back to manufacturer to convert the product ID to resolve this issue. Alternatively, customer may wait for next release in which this issue will be resolved.

CSCsm51669 BR1310 Crashes When WEP Key Is Improperly Configured

Symptom WMIC Cisco 3201 (in WGB or NRB station role) crashes When WEP Key is Improperly configured for some scenarios, traceback occurs using shared key authentication with WEP. If the AP (or RB) and WGB (or NRB) are both configured with encryption mode wep mandatory, no traceback occurs. All other encryption mode combinations (no encryption, mandatory, optional) between AP (or RB) and WGB (or NRB) may cause a traceback.

```
CONFIGURATION EXAMPLE (encryptional wep optional)
int d0
encryption mode wep optional

CONFIGURATION EXAMPLE (encryptional wep mandatory)
int d0
encryption mode wep mandatory
encryption key 1 size 40bit 0 1111111111 transmit-key
```

Conditions The problem only occurs on the WMIC Cisco 3201 using shared key authentication with WEP.

Workaround Use more robust security settings, e.g EAP based authentication (and encryption).

CSCsm53004 Issues in CISCO-DOT11-ASSOCIATION-MIB

Symptom cDot11ClientCurrentTxRateSet" always returns 1, even though the current rate is other than 1. "cDot11ClientRadioType" returns "unknown" when authentication algorithm is Open or Shared with eap or mac. "cDot11ClientSubIfIndex" returns wrong index value when authentication algorithm is Open or Shared with eap or mac. cDot11ClientDevObjectID always returns "nullOID". "Clients Associated" always returns 0, even though the client is associated with AP.

Conditions These issues are seen when using SNMP get operation.

Workaround There is no workaround.

CSCsm55326 Issues in CISCO-DOT11-SSID-SECURITY-MIB

Symptom The mib object, cdot11SecAuxSsidInfraStruct, can not be set to value (3) from value (1), it shows error and vice versa. For object "cdot11SecSsidMaxBackupVlans", SNMP set operation accepts the value but does not set it.

For read-write object "dot11SecLocalAuthServerEnabled", configuring through SNMP returns error: Error code set in packet - COMMIT_FAILED_ERROR: 1.

For object "cdot11SecAuxSsidProxyMobileIp", SNMP set does not reflect in configuration.

For read-create object "cdot11SecSsidInformationElement", configuring through CLI works fine. However, if we try to set through SNMP, it does not work.

For read-create object "cdot11SecAuxSsidAuthKeyMgmt", configuring through CLI works fine. However, if we try to set through SNMP, it does not work.

Conditions For the object "cdot11SecAuxSsidWpaPsk", always returns NULL. These issues are seen when using SNMP get or set operations.

Workaround There is no workaround.

CSCsm57073 Issues in authentication with Eap, Mac in CISCO-DOT11-SSID-SECURITY-MIB

Symptom The following mib objects can not be set from SNMP:

```
cdot11SecAuxSsidAuthPlusEap
cdot11SecAuxSsidAuthEapMethod
```

The following mib objects does not work consistently from SNMP set operations:

```
cdot11SecAuxSsidAuthMacMethod
cdot11SecAuxSsidAuthMacAlternate
```

The following mib objects can be set from SNMP, but not from CLI: cdot11SecAuxSsidAuthPlusMac.

Conditions For the object "cdot11SecAuxSsidWpaPsk", always returns NULL. These issues are seen when using SNMP get or set operations.

Workaround There is no workaround.

CSCsm72668 MIBS file and SNMP Issues in C320x WMICs

Symptom The following mib object can not be set correctly for Cisco 320x radios: cdot11SecAuxSsidAuthEnabled.

The following mib objects show wrong values for Cisco3202 radios:

```
cd11IfPhyDsssMaxCompatibleRate,
cd11IfPrivacyOptionMaxRate,cd11IfSuppDataRatesPrivacyValue.
```

The following mib object can not be set correctly for Cisco 3202 radios:

```
cd11IfPhyDsssMaxCompatibleRate.
```

The following mib object can not be set correctly for Cisco 3202 and Cisco 3205 radios:

```
cd11IfPreambleType, cd11IfVlanEncryptionMode.
```

The following mib objects show wrong values for Cisco 3205 radios: cd11IfRfFrequencySpacing, cd11IfRfFrequencyBandType.

Conditions For the object "cdot11SecAuxSsidWpaPsk", always returns NULL. These issues are seen when using SNMP get or set operations.

Workaround There is no workaround.

CSCsm74538 MAR has different sensitivity limits based on Power Level of Hammer 4_9

Symptom The sensitivity of Cisco 3202 measured by 1524 has different values at different transmit power levels. There is an 8 dB difference in measured sensitivity at Power levels of PL1 and PL5.

Conditions The difference in measured sensitivity is worst at 6 Mbps.

Workaround There is no workaround.

Related Documentation

Your product shipped with a minimal set of printed documentation. The full set of documentation is available online at:

http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html

Cisco 3200 Series Router–Specific Documentation

Unless otherwise specified, the following documentation is available at Cisco.com at **Support > Routers > Cisco 3200 Series Wireless and Mobile Routers**:

- *Cisco 3200 Series Router Product Release Notes*—This document. It provides caveats and information on accessing documentation and obtaining technical assistance for the Cisco 3200 Series Router.
- *Radio Channels and Transmit Frequencies*—Description of how to determine the radio type and how to configure radio channel spacing, radio channel or frequency, and Dynamic Frequency Selection (DFS).
- *Roles and the Associations of Wireless Devices*—Description of the roles Cisco wireless devices can be assigned and how the role of a device affects its ability to associate or not associate with other wireless devices.
- *Cisco 3200 Series Router Hardware Reference Guide*—Descriptions of the Cisco 3200 Series Mobile Access Router enclosures and mobile interface cards.
- *Cisco 3200 Series Wireless MIC Software Configuration Guide*—Example procedures for using the Cisco IOS commands to configure the Cisco Wireless Mobile Interface Card (WMIC).
- *Configuration Guide for the Cisco 3200 Series Router*—Sample procedures for using the Cisco IOS commands to configure assembled Cisco 3200 Series Routers.
- *Cisco 3200 Series Mobile Access Router Reference Sell Document*—An overview of the reference sell program and components for the Cisco 3200 Series Routers.
- *Cisco 3200 Rugged Enclosure Assembly Guidelines*—Guidelines for adding or removing cards from the Cisco 3200 Router MIC stack in the Cisco 3200 Rugged Enclosure Assembly at:
http://www.cisco.com/en/US/partner/products/hw/routers/ps272/prod_technical_reference_list.html
This is a restricted document that requires a CCO password to access.
- *IOS Release Notes for the Cisco 3200 Router*—The enhancements to and caveats for Cisco IOS releases as they relate to the Cisco 3200 series router at:

http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html

Recommended Reading

The following URLs, books, and other sources provide general discussions of topics that apply to the Cisco 3200 series router, such as radio wave propagation, WLAN security, and network design:

- Cisco Wireless LAN Security Overview
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html
- Cisco Network Admission Control for Wireless LANs
http://www.cisco.com/en/US/products/ps6521/prod_brochure0900aecd80355b2f.html
- White Paper: Cisco IOS Reference Guide (Document ID: 15166)
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- *802.11 Wireless LAN Fundamentals*, ISBN 1-58705-077-3
- *Fundamentals of Wireless LANs Companion Guide*, ISBN 1-58713-119-6
- *802.11 Wireless Network Site Surveying and Installation*, ISBN 1-58705-164-8
- *Deploying License-Free Wireless Wide-Area Networks*, ISBN 1-58705-069-2
- *Network Security first-step*, ISBN 1-58720-99-6

The [Cisco 3200 Series Mobile Access Router ATP Partner Site](#) provides a variety of marketing and technical information. You must be an Authorized Technology Provider (ATP) partner for the Cisco 3200 Series Mobile Access Router to access this site.

Tools and Web Sites

If you are a registered Cisco Direct Customer, you can access the following websites:

- *Cisco IOS Command Lookup*—A search engine dedicated to finding information on Cisco IOS commands in the *Cisco IOS Command Reference*, *Cisco IOS Configuration Guide*, *Catalyst Command Reference*, and *PIX Firewall Command Reference*.
<http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl>
- *Bug Toolkit*—Searches for known bugs, based on software version, feature set, and keywords. The resulting matrix shows when each bug was integrated or fixed, if applicable.
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
- *Feature Navigator*—Locates the Cisco software release, based on the features that you want to run on your network.
<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>
- *Software Advisor*—Provides information on compatibility of hardware products and software releases at the following URL:
<http://tools.cisco.com/Support/Fusion/FusionHome.do>

Web pages for specific parts are listed at appropriate places in this technical reference. See [Table 1](#) for a list of Cisco 3200 Series Mobile Access Router part manufacturers and their home pages.

Table 1 *Web Pages of Cisco 3200 Series Mobile Access Router Part Manufacturers*

Manufacturer	Web Page
Intel	www.intel.com
Freescale Semiconductor	www.freescale.com
Maxim	www.maxim-ic.com
Micron Technology	www.micron.com
Xilinx	www.xilinx.com
AMP/Tyco	www.tycoelectronics.com/components
Linear Technology	www.linear.com
Infineon	www.infineon.com
Broadcom	www.broadcom.com
Elantec	www.elantec.com
Texas Instruments	www.ti.com
Altera	www.altera.com

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.